# *It's Not About the Technology: Enabling E-Signatures for E-Government*

Maryland IT Security and Privacy Conference

Stephen H. Holden

Holden@umbc.edu

UMBC Department of IS

UMBC

AN HONORS UNIVERSITY IN MARYLAND

# Outline

- Context for E-signatures in E-Government
- Context for E-signatures at the IRS
- Policy & Technical Considerations
- Change Management Considerations
- Implications for E-government
- Possible Next Steps

Research funded, in part, by the IBM Center for the Business of Government

# Context for E-signatures in E-Government

- Usually need signature to comply with legal or policy requirement
- Not necessarily e-authentication
- Necessary to move to higher level e-government
- Imperative to address user concerns with security and confidentiality

UMBC
AN HONORS UNIVERSITY IN MARYLAND

# Context for E-signatures at the IRS (History)

- Historical reliance on paper signatures for tax returns
- Agreement in Congress, Treasury and IRS of need to eliminate paper signatures
- Started with Telefile
- E-file now half of individual returns; E-sign now ¾ of e-file

# Context for E-signatures at the IRS (Business)

- IRS had studied eliminating paper signatures for years
- Lots of organizations thought they had a role
- New ETA organization provided focus, vision and authority
- New perspective on risk reward tradeoff
- Activity-based costing confirmed cost of processing paper signature documents
- Executive support up to Commissioner

# Context for E-signatures at the IRS (Policy)

- Tax returns must be signed
- Discretion to define “signing”
- Support in Congress
- IRS consolidated policy development and oversight in ETA
- Separated signatures (legal requirement) from authentication (business requirement)

# Context for E-signatures at the IRS (Partnership)

- Third parties play significant role in e-file product development and delivery
- IRS sought private sector help to address paper signature problem
- Agreement on goal; business/technical solution less clear
- Inter-agency work group adapted state model with private sector participation

# E-signatures in the IRS e-file Program

| *Year/ Filing Channel* | *1999* | *2000* | *2001* | *2002* | *2003* |
|---|---|---|---|---|---|
| **On-line: ECN** | Previous year tax prep software | Previous year tax prep software | | | |
| **On-line: Self-Select PIN with Knowledge-based Authentication** | | | Validate AGI Total Tax Birth date (reject if wrong) | Validate AGI Birth date (reject if wrong) | Validate AGI Birth date (reject if wrong) |
| **Preparer: Practitioner PIN** | Selected EROs | Selected EROs | | Selected EROs | All EROs |
| **Preparer: Self-Select PIN with Knowledge-based Authentication** | | | Validate AGI Total Tax Birth date | Validate AGI Birth date | Validate AGI Birth date |

**Table 1 Electronic Signature Program Features by Year**

UMBC
AN HONORS UNIVERSITY IN MARYLAND

**www.umbc.edu**

# E-signature Program Results

| Filing Season | Telefile | Practitioner PIN | Government-issued-PIN (ECN) | On-line Self-Select PIN | Preparer Self-Select PIN | Total e-sign | Total e-file | Percent e-sign | Percent e-sign no Telefile |
|---|---|---|---|---|---|---|---|---|---|
| **1999** | 5,664 | 500 | 660 | | | 6,824 | 29,345 | 23.3% | 4.9% |
| **2000** | 5,154 | 5,423 | 1,416 | | | 11,993 | 35,381 | 33.9% | 22.6% |
| **2001** | 4,411 | | | 4,222 | 4,678 | 13,311 | 40,244 | 33.1% | 24.8% |
| **2002** | 4,176 | 14,833 | | 6,801 | 2,768 | 28,578 | 46,892 | 60.9% | 57.1% |
| **2003** | 4,023 | 21,641 | | 8,530 | 2,365 | 36,559 | 52,194 | 70.0% | 67.5% |
| **2004** | 3,757 | 29,452 | | 10,593 | 1,131 | 44,933 | 59,689 | 75.3% | 73.6% |
| As of 4/27/2004 | | | | | | | | | |

UMBC
AN HONORS UNIVERSITY IN MARYLAND

www.umbc.edu

# Policy and Technical Considerations

- Match the tool to the task
  - Don't authenticate if you only need signatures
  - Don't require "strong" authentication unless business needs require it
  - Don't specify burdensome or complex solutions that are beyond the capability of your user base
- Leverage the resources you have
  - Many government organizations have long-standing relationships with users that can facilitate e-signatures and e-authentication
  - Third parties may be also have long-standing relationships built on trust and experience

# Change Management Considerations

- Public law and policy can be enablers
- Revise, if at first you partially succeed
- Establish business ownership of e-signature & authentication efforts
- Partner, partner, partner
- Provide or obtain executive sponsorship

UMBC
AN HONORS UNIVERSITY IN MARYLAND

# Implications for E-Government

- A combination of factors brought about e-signatures for the IRS
- Eliminating paper is as much about change management as IT
- Agreement on common business goals is crucial
- If the IRS can do it, so can you!

UMBC
AN HONORS UNIVERSITY IN MARYLAND

# For more reading on this topic


- Holden, S.H. (2004) Understanding Electronic Signatures: The Key to E-Government. Washington, DC: The IBM Center for the Business of Government.
- Millett, L. I. and Holden, S. H. (2003) Authentication and Its Privacy Effects. IEEE Internet Computing November/December 2003: 54-58.
- Computer Science and Telecommunications Board, National Research Council. (2003). Co-author of Who Goes There? Authentication Through the Lens of Privacy. S.T. Kent and L.I. Millett (eds.) Washington, D.C.: National Academy Press.

# Possible Next Steps

- OMB e-Authentication Policy--Five Step Process for Determining Desired Assurance Level and Related Authentication Solution
  1. Conduct risk assessment
  2. Map identified risks to assurance level (Four levels)
  3. Select technology based on NIST technical guidance
  4. Validate that implemented system has achieved desired assurance level
  5. Periodically reassess system to assure solution produces desired assurance.

# Five Step Process for Determining Desired Assurance Level

- OMB e-authentication policy
  1. Conduct risk assessment
  2. Map identified risks to assurance level
  3. Select technology based on NIST technical guidance
  4. Validate that implemented system has achieved desired assurance level
  5. Periodically reassess system to assure solution produces desired assurance.

# E-Government System Risk Assessment (Step 1)

- System Description
  - Volume of Users
  - Types of Users
  - Characteristics of Users
  - Third party intermediaries?
  - Existing technical, management or policy controls in place for risk mitigation
- Potential impact:
  - Inconvenience, distress or damage to standing or reputation: Financial loss or agency liability: (Low, Moderate, High)
  - Harm to agency programs or public interest: (Low, Moderate, High)
  - Unauthorized release of sensitive information: (Low, Moderate, High)
  - Civil or criminal violations: (Low, Moderate, High)
  - Likelihood of harm or impact: (Low, Moderate, High)
  - Presumed Assurance level: (**1-4)**

# Mapping Risks to Assurance Levels (Background for Step 2)

- Two factors
  - Potential harm or impact (Selected examples to follow)
    - Low
    - Moderate
    - High
  - Likelihood of harm or impact
    - Low < 30 percent
    - Moderate >30 and < 70 percent
    - High > 70 percent

UMBC
AN HONORS UNIVERSITY IN MARYLAND

# 4 Levels of Assurance (Level 2 (Background for Step 1)

- **Little or no confidence**
- **Some confidence**--An agency employee has access to potentially sensitive personal client information. She authenticates individually to the system at Level 2, but technical controls (such as a virtual private network) limit system access to the system to the agency premises. Access to the premises is controlled, and the system logs her access instances. In a less constrained environment, her access to personal sensitive information would create moderate potential impact for unauthorized release, but the system's security measures reduce the overall risk to low.
- **High confidence**
- **Very high confidence**

# Impact Examples for Agencies (Source: OMB Policy as Background for Step 2)

Potential impact of ***unauthorized release of sensitive information***:

**Low—**at worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact (i.e., **limited** adverse effect on organizational operations)

**Moderate—**at worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact (i.e., **serious** adverse impact on organizational operations).

**High**—a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact (i.e., **severe or catastrophic** adverse effect on organizational operations).

# Potential Impact Categories for Authentication Errors

## OMB E-authentication Policy as Background for Step 2

| | Assurance Level Impact Profiles | | | |
|---|---|---|---|---|
| **Potential Impact Categories for Authentication Errors** | 1 | 2 | 3 | 4 |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | High |
| Financial loss or agency liability | Low | Mod | Mod | High |
| Harm to agency programs or public interests | N/A | Low | Mod | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | High |
| Civil or criminal violations | N/A | Low | Mod | High |

# NIST Special Publication 800-63

## (Background for Step 3)

- Published June 2004
- Revised from proposed version based on extensive public comment
- Complements OMB e-Authentication policy
- Technical requirements for each level of assurance for:
  - Tokens
  - Identity Proofing
  - Remote Authentication Mechanisms
  - Assertion Mechanisms
- Important points:
  - Authentication technology works with policy and process to produce authentication solution
  - Totality of authentication solution mitigates risks